*"RFID" access airport gate* (handwritten)

| L35 | L31 and @ad<=20031126 | 108 | L35 |
|---|---|---|---|
| L34 | ('5390880'\| '6141607'\| '5437422'\| '5828979'\| '6459964'\| '5798949'\| '6662141'\| '6304801'\| '6873962'\| '5440489'\| '4266273'\| '4752053'\| '4617627'\| '5239472'\| '5006847')[URPN] | 108 | L34 |
| L33 | ('4179739')[URPN] | 15 | L33 |
| L32 | L29 and (train$ or locomotive) and (wheel$ same (correct$ with (factor or coefficient))) | 1 | L32 |
| L31 | ('6775690'\| '6860423'\| '6697811'\| '6839753'\| '6750198'\| '6459964'\| '6662141'\| '6304801'\| '6873962'\| '6802003'\| '4752053'\| '5390880'\| '6141607'\| '5239472'\| '5437422'\| '5828979'\| '5006847'\| '5798949'\| '4617627'\| '5440489'\| '4266273') [URPN] | 108 | L31 |
| L30 | ('6408330'\| '4179739')[URPN] | 21 | L30 |
| L29 | 4179739.pn. | 1 | L29 |
| L28 | L27 | 1 | L28 |

*DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR*

| L27 | L26 and access$ and security | 1 | L27 |
|---|---|---|---|
| L26 | L17 and "iclass" | 15 | L26 |
| L25 | L24 and "iclass" | 0 | L25 |
| L24 | L23 and security | 21 | L24 |
| L23 | L17 not l19 | 49 | L23 |
| L22 | l20 not L21 | 5 | L22 |
| L21 | L20 and gate and security | 2 | L21 |
| L20 | L19 and access$ | 7 | L20 |
| L19 | L18 and smart$ | 7 | L19 |
| L18 | L17 and hid$ | 33 | L18 |
| L17 | card and iclass$ | 56 | L17 |
| L16 | card and "iclass16k.cg" | 0 | L16 |
| L15 | hID and "iclass16k.cg" | 0 | L15 |

*DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR*

| L14 | L13 and check$ | 11 | L14 |
|---|---|---|---|
| L13 | L12 and (airport or flight) | 11 | L13 |
| L12 | L11 and (random$ near2 (code or number)) | 45 | L12 |
| L11 | L10 and (password or "pass-word") | 179 | L11 |
| L10 | L9 and (remote$ with access$) | 263 | L10 |
| L9 | L8 and (computer$ with access$) | 713 | L9 |
| L8 | safeguard and security | 2048 | L8 |
| L7 | L6 and ((correct$ or edit$ or chang$) with (coefficient or factor)) | 0 | L7 |
| L6 | L5 and gps | 1 | L6 |
| L5 | 4179739.urpn. | 15 | L5 |
| L4 | ('4179739')[URPN] | 15 | L4 |
| L3 | 4179739.pn. | 1 | L3 |
| L2 | 4179739.pn. and (gps) | 0 | L2 |

☐ ▐ Generate Collection ▌ ▐ Print ▌


L55: Entry 14 of 14                    File: USPT              May 13, 1997


DOCUMENT-IDENTIFIER: US 5629981 A
TITLE: Information management and security system


Abstract Text (1):
A closed loop, (networked) information management and security system which
provides a secure, end-to-end fully automated solution for controlling access,
transmission, manipulation, and auditability of high value information comprising
an RFID transponder badge 302 and an RF reader transceiver 315 which is associated
with a host peripheral or a network. The RF reader transceiver 315 automatically
identifies and verifies authorization of the RFID transponder badge holder via a
"handshake" prior to allowing access to the host peripheral. The energy generated
by the transmission of the interrogation signal from the RF reader means 315
provides a power source which is accumulated and then used to activate a
transponder 304 response from the RFID transponder badge 302. The RF
reader/transceiver 315 writes the access transaction on either the RFID transponder
badge 302 and/or the host peripheral database or the network controller.
Alternatively, the RF reader means 315 may be associated via network server with a
LAN, WAN, or MAN. Optionally, an RFID badge 302a may be powered by an independent
power source such as a flatpak battery 314.

Application Filing Date (1):
19940729


Brief Summary Text (3):
The present invention relates to a complete, end-to-end, automatic transaction
control/monitoring method for transmitting, under variable and high levels of
security, high-value business, personal, or Federal/military information, on a real
or near real-time basis.

Brief Summary Text (5):
A "secure document" or "secure information" is any document media (paper, disc,
voice, video, etc.) containing U.S. classified documents or information (i.e.
"confidential," "secret," "top secret," etc.), business-sensitive, proprietary
documents or information, highly personal documents or information, and any
document or information where limited and fully controlled/auditable access is
desired.

Brief Summary Text (6):
If an individual wishes to send a secure document via telefacsimile, for example,
the current method of sending such a secure document is to call the receiving end
and somehow make sure by voice communication that the intended, authorized
recipient is standing at the other end at the receiving telefacsimile. Once the
identity and proximity to the receiving telefacsimile of the intended recipient
(mainly, via voice familiarity) is verified, the sending individual sends the
document. After sending, the intended recipient provides confirmation to the
sending individuals that the document was printed and received.

Brief Summary Text (7):

The same limited _security_ procedure is followed when printing information from an electronic database to a remote conventional printer or other terminal device.

Brief Summary Text (9):
It is noted that some islands of automation are available, but no end-to-end automation, with full auditability and real-time or near real-time control. Current systems such as a secure telephone unit ("STU") or STU facsimile machines assure no illegal tapping or eavesdropping but do not guarantee that the caller, recipient, or group is positively identified or is an authorized user or recipient. The positive _identification and verification_ of authorization is always performed manually. Thus, there is a need for end-to-end automation, with full auditability and real-time or near real-time control of the transmission of secure documents and information.

Brief Summary Text (13):
Therefore, there is a need in the art to provide a cost-effective automatic room _security_ which mechanizes the room _access_ logs and thereby decreasing costs and increasing productivity.

Brief Summary Text (14):
Exacerbating the foregoing problems, in order to copy certain secret government documents, only certain "secure" or tempest class copiers may be used so that the copier OPC drum may be cleared after copying and cartridges may be disposed of by only authorized personnel. Before these copies are made, a log sheet must be completed providing the details of the copying of the document. This creates yet another labor-consuming delay that increases costs and decreases productivity. In fact, _access_ logs and usage data are generally maintained manually for secure facilities, information handling equipment, and users.

Brief Summary Text (15):
Therefore, there is a need in the art to provide an automatic information management and _security_ system which eliminates the time inefficiencies and waste associated with manual logging and tracking of copies of high-value, secret documents.

Brief Summary Text (16):
Underlying the entire system is the fact that it is up to the employees and _security_ personnel to _verify_ whether a particular individual has a secret clearance, badge code number, or some other indicia of authorization and _identification_. Therefore, to prevent improper _access_, manual or personal direct intervention is required to _verify_ both authorization and need to know in order to prevent improper and unauthorized transfer of secure documents. The _verification_ by employees diverts resources from productive activity. The _verification by security_ personnel results in additional salary or expense overhead.

Brief Summary Text (18):
On a related matter, when an individual's authorization is revoked and the individual gains unauthorized _access_ to secure documents a _security_ breach occurs. When this _security_ breach is manually detected, it is impossible to inform all the employees and/or _security_ personnel of the breach in a timely fashion in order to insure manual intervention. In a large company, timely notification and communication of the changing authorizations of employees is relatively impossible. This is because authorization has traditionally been carried in the form of a color-coded badge or the like. As a result, if the _security_ of a document has been breached by use of an authorization which has been terminated or forged, an entire month or more could pass before the monthly DOD audit discovers the _security_ breach.

Brief Summary Text (19):
Therefore, there is a need in the art to provide an automated system for

continuously updating comprehensive information about the authorizations of individuals, and to prevent unauthorized <u>access</u> to secure documents at the time <u>access</u> is attempted (real-time control).

Brief Summary Text (21):
Therefore, there is a need in the art to provide an automated information management and <u>security</u> system which would be compatible with the present office technology, yet would be compatible with potential integrated office equipment, networks, and architectures of the future.

Brief Summary Text (22):
The present invention provides an information management and <u>security</u> system which overcomes the shortcomings of the known systems providing various advantages such as instantaneous, multiple secure <u>access</u>(es) and minimizing the total "life-cycle" costs of managing "secure" information (from inception to destruction) utilizing present technology while being also compatible with new technology contemplated for the future. Also provides for transaction database services such as archiving, historic usage trends, transaction reporting/abstracting (user-definable) services.

Brief Summary Text (24):
It is in view of the above problems that the present invention was developed. The invention is a closed loop information management and <u>security</u> system which provides a secure end-to-end and automated solution for controlling <u>access,</u> transmission, manipulation, auditability control of classified, mission-critical, high-value information managed by DOD, National <u>Security</u> Agency, other Federal Agencies, businesses, and individuals respectively.

Brief Summary Text (26):
The present invention allows information management to be "transaction based." Each automatic information transaction is built around a sequence such as a positive caller and recipient handshake and identification ("ID"), information upgrade (write) record, configuration control (date, time, location and revision stamp), creation of a transaction summarizing "communication data stream" (e.g., ATM cell, frame) packet, destination ID, additional authentication (e.g., voice signature, biographical identification), send and receive date/time, location stamp, etc. The host computer, network server or network controller maintains this "transaction" log automatically and dynamically maintains information authorization, usage, movement, and an upgrade/change log and foils any unauthorized <u>access</u> or tampering and does any real-time reclassification or declassification as required. As such, this is a "transaction" based system that can be enhanced to add fault tolerance, redundancy, software-based <u>access</u> control algorithm creation, etc. to provide a flexible system.

Brief Summary Text (27):
Briefly, in its most generic sense, the present invention comprises a read/write type radio frequency <u>identification</u> ("RFID" Radio Frequency, InfraRed or optical) means (transponder) and a radio frequency (transceiver) reader ("RF reader") means which is associated with a host peripheral or terminal device wherein the RF reader means passively and automatically <u>identifies and verifies</u> authorization of the <u>RFID</u> means via a "handshake" prior to allowing <u>access</u> to the host peripheral or terminal device or an information network. Preferably, the RF reader means writes the complete transaction via a unique "packet") on the <u>RFID</u> means, and/or the host peripheral or terminal or a network server device. In this fashion, the history of all transactions may be stored on the <u>RFID</u> means and/or host peripheral or terminal device. The present invention may be provided commercially in a "securitization kit" to upgrade existing equipment and information-handling facilities.

Brief Summary Text (28):
In a second aspect of the present invention, the RF reader means is embedded,

plugged-in, connected or associated with the host peripheral or terminal device. Once a transaction is completed the RF reader means may record and write the transaction on the RFID means, and/or the host peripheral or terminal device, and/or a server database connected or associated with the terminal device. Optionally, the RFID means may further include stored biological data in ROM such as digitized voice signature, retina scan, fingerprints, etc. and other analog sensors (temperature, humidity, pressure, etc.) as well as commercially available physical "position" sensors such as Global Positioning System ("GPS"), coastal navigation system (LORAN), or other satellite/magnetic based positioning system. As an added security feature the RFID means may include electronic hardware and/or software encryption means to statically and dynamically "encrypt" the authorized user identification code, information destination, transaction location, time/date, configuration control, and secondary biological user(s) identification.

Brief Summary Text (29):
In a third aspect of the invention the RFID means may be coupled with an independent power source such as a battery.

Brief Summary Text (30):
The RFID means may comprise an integrated ID, memory storage, and a communications device such as a Personal Computer card ("PC card") which conforms to standards promulgated by the Personal Computer Memory Card International Association ("PCMCIA") having an RF transponder, mass memory, 2-way communication port(s) and input/output data means. Optionally, the RFID means has encryption device (Integrated Circuit) means to encrypt the output data. In addition, the RFID has unique biographical information patterns in Read Only Memory (ROM) for "static" information and "dynamic" position, time, place, date information.

Brief Summary Text (31):
In one preferred embodiment, the RFID means is electronically similar to the "bullet" or flat-pack card disclosed in U.S. Pat. No. 5,053,774 to Schuermann et al., which is hereby incorporated by reference in its entirety.

Brief Summary Text (32):
The RF reader means is preferably an RFID reader module which comprises a plug-in PC card having a communication antenna, an RF module, a control module, and input/out data means. Optionally, the RFID reader means comprise data packetization means, encryption means and bus control means.

Brief Summary Text (33):
The invention provides an advantage by minimizing overall life-cycle-cost to manage high value information from its inception to the end of its usefulness. The invention also provides an advantage by allowing real-time, dynamic classification of information in case of a security breach or authorization changes (levels, users, time, place, etc.).

Drawing Description Text (5):
FIG. 3a illustrates in greater detail a passive, user "read/write" type RFID badge suitable for the user segment of the information management and security system;

Drawing Description Text (6):
FIG. 3b illustrates an "active" user RFID badge of FIG. 3a and a battery to enhance speed and range of the ID device and the transaction;

Drawing Description Text (8):
FIG. 4 illustrates one transaction packetization scheme suitable for use in said information management and security system; and

Drawing Description Text (9):
FIGS. 5A and 5B illustrate a general hardware layout in a specific high-value

printing cartridge refurbishment application of said information management and security system.

Drawing Description Text (10):
FIG. 6 illustrates a specific application of said information management and security system utilizing technology from the cellular communications industry.

Detailed Description Text (3):
To provide an overview, in its most generic sense, the present invention comprises an RFID means and a radio frequency reader ("RF reader") means which associated with a terminal device or other equipment such as a lock mechanism, wherein said RF reader means automatically interrogates said RFID means which responds by broadcasting identification so that said RF reader means identifies and verifies authorization of the RFID means and either stores a record of the transaction or communicates a record of the transaction to a server database prior to allowing access to the terminal device or other equipment.

Detailed Description Text (6):
The user segment is comprised of individuals wishing to send and receive information such as secure documents. For the user segment, the present invention requires intelligent identification means, preferably RFID means as stated above. The RFID means may be any device which allows positive identification of the wearer and which provides an ability to communicate with the single or multiple host/network equipment(s) or facility segment(s).

Detailed Description Text (7):
The term "terminal device" is broadly defined as any type of electronic equipment or hardware, e.g. printer, copier, pager, personal computer (PC), facsimile machine, work stations, video, terminal, telephone, VCR, radio, electronic door mechanism, mass memory storage device, data storage device for storing log data, modem, etc. Preferably, the RF reader means provides identification security and then writes the transaction on the (portable or fixed) RFID means and/or a server database connected or associated with the terminal device or other equipment. Further, the history of all transactions may be stored on the RFID means and/or server database. The present invention may be provided commercially in a "securitization kit" to upgrade existing facilities.

Detailed Description Text (8):
In the preferred embodiment, such identification means is preferably in the form of a user RFID badge transponder (hereinafter "RFID badge" or "RFID transponder") or security badge. Such an "RFID transponder" is an active or passive read only or read/write transponder which operates via radio frequency means, infrared means, or other optical means at a low, high or auto-frequency.

Detailed Description Text (9):
Under the present invention, the user segment, at least a group of individuals, wears an intelligent, passive user RFID badge. It is noted that the present invention does not require additional inconvenience on the part of the user segment as wearing dumb ID badges is a fact of life in the defense and business world wherein security clearances are written on badges manually. Thus, the user RFID badge aspect of the invention is an improvement over current technology because security clearance information need not be physically visible for the public to read.

Detailed Description Text (10):
Such a user RFID badge is illustrated in FIGS. 3a and 3b. The uses of each type of user RFID badge are more fully set forth in examples 1 and 2. Both user RFID badges (passive) shown generally at 302 and 303 (active, with battery) commonly include a Personal Computer card ("PC card") which conforms to standards promulgated by the Personal Computer Memory Card International Association ("PCMCIA") having an RF

read/write transponder 304, application-specific, electronic mass memory 308, transponder antenna (screened on) 306, and input/output data means 312. Optionally, the input/output data means 312 includes unique encryption (hardware or software) means 313 to decrypt input data and encrypt the output data/packets etc. via a specialty crypro Application Specific IC (ASIC) in the form of a random number generator chip or utilizing hardware or software "crypto keys" for information/date encryption which is user-definable. Optionally, the user RFID badge 310 can also store a person's unique biological digitized data in Read Only Memory ("ROM") 310 for enhanced authentication purposes, e.g. digital voice signature, digitized fingerprints, or digitized eye retina prints, etc.

Detailed Description Text (11):
With reference to FIG. 3b, the user RFID badge shown generally at 302a uses the PC card 303 of FIG. 3a and is physically and electrically joined to a flatpak battery power source 314. Applications specific to this user RFID badge 302a are more fully explored in Example 2.

Detailed Description Text (12):
With reference to FIG. 3c, the equipment or facility segment of the present invention requires an RFID reader means which may be of plug-in or built-in type. The RF reader means is defined as a multi-frequency, range-adaptive radio frequency transceiver preferably in the form of an RFID reader module shown generally at 315 which comprises a plug-in PC card 317 having a control module 316 for controlling an RF module 318 connected to a communication antenna 320, and having input/output data means 322. Optionally, the RFID reader means comprise integrated circuits (ICs) such as data packetization means 321, encryption means IC 324 and bus control means 326 possibly connected via modem (wired or wireless) to the network server.

Detailed Description Text (15):
The network segment requires some type of host hardware to handle and manage the information and security system. The host hardware functions to authenticate authorized user IDs, track roaming user locations, and control configuration of the system as well as revisions in any aspects of control. The network segment also can perform compression or decompression of data, control local area network and wide area network applications, provide a "throttle" in that it could provide a variable transaction "packet" creation/transfer rate of control, provide encryption means and provide multi-user and equipment daisy chaining (add/drop, change priority, etc.). In its management aspect, the network segment can provide functions such as billings, generate reports relating to general usage trends, provide an audit-trail of each/user-defined transaction, control classification and reclassification of both documents and authorized users, provide point-to-point or point-to-multipoint "broadcast" transactions, provide secure communications for roaming users, and other application specific features, such as an automatic/date/time/location stamp for every transaction wherein the location stamp utilizes dynamic code(s) such as GPS location code or "variable" facility codes for added security.

Detailed Description Text (17):
The unique portion of the present packetization scheme is that the location stamp showing the authorized origination and destination(s) of the request is encoded and encrypted. This aspect is critical in the sense of preventing unauthorized entry in a control area. If a person attempts unauthorized entry by using a location code obtained by copying airborne transmissions or stolen badge, etc., access is denied first because the person is unauthorized and second because an authorized user also has a limited number of locations in which transactions are authorized. Information relating to the limited number of authorized locations is stored in a look up table of the host computer or the network server and can be dynamically updated as required for additional security.

Detailed Description Text (18):
It should be emphasized that in FIG. 4, Authorized User ID, Destination, and

Recipient IDs are all encrypted, even in the header, using a <u>random number</u> scheme described below, or some other similar scheme. Thus, even if unauthorized personnel obtains the transmitted packet, the unauthorized personnel would be unable to decrypt or decode the packet to obtain the real code, and even if the real code is obtained, the host or network server could dynamically change the location code on an everyday basis to foil unauthorized copying or pirating of the code.

Detailed Description Text (20):
With respect to encryption of data, a decoding or decryption approach attempted by unauthorized users of RF, broadcast user ID/voice signature or other personally unique data is the capture and duplicate approach. One way to combat this approach is to deploy a "<u>random number</u> seeding" algorithm to continually and very frequently change the "ID data".

Detailed Description Text (21):
This encryption algorithm may be embedded in the transponder device (<u>RFID</u> or Infrared or optical ID) itself or in a separate encryption chip or integrated encryption/packetization chip. A short series of transmitted transactions below the RF equipped "object" under protection and the other RF technology identification device could be as follows: ##STR1##

Detailed Description Text (22):
It is noted that the user identification code may contain authorized location codes, coded by simple assignment or the Global Positioning System ("GPS") convention of latitude and longitude, which may be merged into the user identification code itself and may be changed and/or encrypted. As a result, both standing data and dynamic data exists in the identification code, the mix and frequency of change of which is dependent upon the level of <u>security</u> desired. This dynamism is critical to maintaining extremely high levels of <u>security</u> in the system. In the event the user identification code carried by the <u>RFID</u> badge is copied in order to gain unauthorized <u>access</u> to information from a location different from that originally authorized (e.g. a computer hacker, misuser/abuser attempting <u>access</u> to secure information or documents via modem), this <u>access</u> would be denied. This packetization scheme combining static code and dynamic code which is controlled and changed according to some predetermined algorithm by the controller or the network server based on the requirements of the using community appears unique as past schemes appear to take static data and recombine the data "on the fly."

Detailed Description Text (24):
The badge system also provides enhanced <u>security</u> under the present invention. If an individual's badge is stolen, the individual simply calls the network management people regarding the stolen badge. The network management people drop the badge from the authorized user list. Therefore, the present invention can provide real-time configuration control and <u>security</u> control.

Detailed Description Text (25):
The equipment or facilities segment may include an application specific memory (ASM), which is preferably a mass-memory plug-in card, which is not absolutely required for operation of said information management and <u>security</u> system. A suitable card would contain at least forty megabytes of storage capacity and would be characterized by multi-page, user-definable, mapping/layout, input/output, mass memory devices of silicon, gallium arsenide or a hybrid material. This additional ASM could be used to store additional transaction history data as desired. Further uses of this card are set forth in greater detail below.

Detailed Description Text (26):
The present invention also has applications in paging and/or telephone transactions wherein a central office telephone switch (wireline or cellular) has the present invention installed in the switch. When a secure voice transmission is required, a

central office switch may store an individual's voice signature in its database for comparison and verification of identity.

Detailed Description Text (27):
With respect to wireless telephonic transactions, central switches have base stations so that with a cellular phone, repeaters transmit the cellular phone signal to the next cell. The cordless/cellular phone itself and/or base station equipment can have RFID readers of the present invention installed as well as other authorization data such as digitized voice bio-signature data.

Detailed Description Text (31):
Specific applications exist utilizing a user RFID badge having no battery. Such a badge is illustrated in FIG. 3, wherein a badge comprises a PC card having a read/write transponder, a flat antenna, application specific mass-memory, and a chip performing input/output functions, preferably including an encryption scheme. Such an RFID badge may be patterned after the "bullet" described in the '774 patent. Because this badge has no battery, its transponder is of limited range. The user RFID badge derives its power by capturing the energy from RF signals generated by the interrogating RF reader module, and, once a predetermined amount of energy is stored, transmits a coded RF signal in a short transmission burst. This method of RF signal transmission is more fully discussed in the '774 patent described above. This badge integrated RFID/communication badge is approximately the physical size of a regular credit card. A second type of user RFID badge discussed more fully below in Example 2 adds a power source such as a battery.

Detailed Description Text (32):
It is noted that either of the above-described user RFID badges could also include a biological or voice signature in ROM. This information stored in ROM could also be encrypted. All encryption could be performed using any of the encryption means currently available on the market, but preferably based on a random number scheme for complete security.

Detailed Description Text (33):
FIG. 2 illustrates a scenario in which there is a user RFID badge in the user segment, and an RF reader that reads the transponder of the RFID badge in the equipment segment. The equipment has a RF reader embedded or plugged into, for example, a fax machine. As person wearing the user RFID badge approaches the fax machine, the RF reader will read the RFID badge when it comes within reading range, probably a meter or less (for passive). When the person's RFID badge is read, the person's RFID badge makes an automatic handshake with the equipment or facility segment so that the equipment, here a fax machine, recognizes that proximate person corresponds to the identification number on the badge.

Detailed Description Text (34):
As a concrete example embodying FIG. 2, secretary A who is attempting to send a secure document to secretary B, does not have to wait for secretary B to be present before the document is placed in the fax machine. As secretary A approaches the fax machine, the RFID reader interrogates secretary A's user RFID badge and determines the identity of secretary A. When secretary A attempts to send the secure document, the fax machine (the host peripheral) initializes the information transfer request and provides configuration control in the form of a date, time, and location stamp. The fax machine checks in a look up table (located either in a module in the host peripheral/fax machine or by sending a query to the network server) to validate and authorize the information transfer request.

Detailed Description Text (35):
Because the host or network automatically has stored a database of authorized people who are authorized to send facsimiles or handle secure facsimiles at this location, the host or network will verify that secretary A is authorized to send a secure document via a handshake between the RFID reader and secretary A's RFID

badge.

Detailed Description Text (36):
Once secretary A sends the document, the network does not transmit the secure
document to the receiving facsimile machine. Instead, the network will store the
document electronically in the buffer of the receiving fax machine or at the
network buffer. At this point, the network can send an indication to authorized
secretary B or other authorized recipient(s) at this location that a secure
document is waiting to be retrieved. This indication can come in the form of a
light appearing on the fax machine, a flashing light on her telephone, or a note on
the computer screen, or a combination of any of the foregoing. This aspect is
critical to security because the secure document is not automatically printed when
secretary B is not present. At secretary B's convenience, secretary B will go to
the fax machine. As secretary B approaches the machine, when proximity to the
machine permits, a handshake between secretary B's fax machine reader and secretary
B's RFID badge will occur. The fax machine will recognize that secretary B is the
authorized recipient and has a secure document ready for receipt. At this point, if
secretary B's RFID badge or the system utilizes the additional biological or voice
signature security feature, the facsimile machine may ask secretary B to say the
name or provide a finger for reading or an eye retina for reading. This additional
step guarantees that the person wearing the badge is in fact secretary B. After
identification is verified, the fax may once again revalidate with the network
server the authorization of secretary B to receive the fax and the fax is printed
and all transaction details and records are updated automatically.

Detailed Description Text (41):
Specific applications of the present invention exist utilizing a user RFID badge
having an independent power source. Thus the user RFID badge of the present example
comprises a PC card having a read/write transponder, a flat antenna, application
specific mass-memory, and a chip performing input/output functions, preferably
including an encryption scheme, and an independent power source. While a user RFID
badge having an independent power source has all the specific applications
described in Example 1 above, addition of the independent power source would create
improvements in those specific applications (i.e. speed, improved reading range)
and creates additional applications described below.

Detailed Description Text (42):
A suitable power source is a battery, preferably a common flatpak battery as shown
in FIG. 3. This battery is physically glued or welded and electronically connected
to the user RFID badge. The addition of a battery transforms the badge into an
active, long-range, fast write transponder. Such a battery would increase the range
of the transponder up to five times that of the original battery. In addition, such
a battery would enable the "read/write" processes in the badge to function faster.

Detailed Description Text (43):
The security badge itself could also be a pager. The badge could be secured
physically and electronically to a pager that is carried on the belt or a pocket.
Accordingly, the pager would incorporate security features not found in the present
paging system.

Detailed Description Text (45):
As alphanumeric pagers are more prevalent, and two-way paging becomes a possibility
in the near future, the present invention provides a security feature which allows
secure messages to be sent without worrying whether an unauthorized person had
access to the page. One of the keys to secure messaging is encryption software
which is laid on top of the conventional signal. Encryption (selective polling)
allows a sender to control who receives a secure page and, more importantly, who
does not receive same.

Detailed Description Text (46):

A powerful aspect of the present invention relies on the ability of the user RFID badge to provide a location stamp. Because a user RFID badge with a flatpak battery has a fairly long range, any secure document carried by an RFID badge carrying person into an unsecured portion of a building can be tracked. Specifically, if one walks away from the document in one part of the building to the next, and if the document is not re-registered automatically (via another RFID reader means), then alarms, flags designed to go up in the network, will prompt security measures to check on the status of the document. This can be accomplished by creating (manually or automatically) an electronic message or page, and sending it over the network to the recipient pool. Accordingly, control over various documents is virtually real-time in determining whether a secure document is in possession of the authorized user or is alternatively replaced.

Detailed Description Text (47):
Another aspect of the present invention is that authorization codes, statuses and user-sets for access for certain locations may be dynamically changed.
Specifically, when a person is working on a secure project for an extended period or specific period of time, wherein the person will have to travel from his or her home building A to buildings B and C or other remote authorized locations for an extended period of time or fixed period of time, the authorization for the person's entry into buildings B and C can be changed dynamically to allow access to both the buildings as well as any equipment therein. When that time expires, or the project is completed, the network automatically cancels the person's authorization to enter buildings B and C. It should be noted that global positioning system technology may be used to enhance the security system as an added feature in order to avoid having to create additional partitions or walls or other means of blocking access within a particular building.

Detailed Description Text (48):
Added applications of the user RFID badge of the present example of the present invention is that multiple users in a given geographical locus (e.g. a building) may be "daisy chained" meaning associated so that multiple users may receive a common message. More specifically, transponders associated with each of the user RFID badges could be configured in a daisy chain. The effect of this is that every time a message comes relative to one user, the same message can be broadcast or simulcast to the other users. The rationale behind this type of configuration of transponders is for purposes of convenience and effective communication.

Detailed Description Text (50):
Because the present invention is transaction based, the system may be used to provide security services to an equipment or building which can be billed to the user on a "per-use" basis. Accordingly, a summary of transactions may also be used for billing purposes because each security transaction could potentially also be a toll producing or toll accounting situation. Additional services which could also be toll producing would be options such as point-to-point transaction, multi-cast or broadcast transactions, or roaming features.

Detailed Description Text (54):
Other applications include, but are not limited to integrated user, information and equipment or asset control; equipment calibration control and auditability control; a professional (lawyer, doctor, accountant, etc.) user information security system; information management and security in the pharmacy field as mandated by the FDA (e.g., controlled substance prescriptions tracking); security over personal property; and auditability and configuration control over the testing of products, production and test equipment to track UL, safety, OSHA, quality, FAA, FDA, etc. compliance.

Detailed Description Text (55):
It is noted that the above-disclosed information management and security system of the present invention may be provided commercially as a service on a "pay-per-use",

i.e. transaction, basis.

Detailed Description Text (59):
In order to prevent unauthorized refurbishing, this unique application of the
present invention requires three main elements: (1) an RFID reader 508; (2) an RFID
transponder 512; and (3) an external mass-memory 516 for storage of transaction
data in the network server 502, peripheral 506 and/or in pluggable integrated
circuit cards commonly known in the industry as PC cards. The RFID reader 508 may
be embedded or plugged into the host printer/copier/fax/scanner and/or the
refurbishing equipment.

Detailed Description Text (60):
With respect to an electronic, secure, tamper-proof transponder, such a transponder
identification device 512 must be imbedded or attached into an insertable, reusable
and disposable electrophotographic printing cassette 510 and/or "after market"
toner/developer dispensing containers for further control. The transponder
identification device 512 is preferably one of the following types: contact type or
close proximity type (e.g., a Dallas semi, IC-type button or proximity "read"
relay); a contactless, RFID device (e.g., a "TIRIS" read-only, read/write and
programmable-type device, with a built-in time, date and place stamp capability and
resident read-only memo/mass-memory)..

Detailed Description Text (61):
The RFID transponder device 512 may also have a built-in temperature, humidity,
oxygen, smoke particle, or ozone sensor, shown at 514, or a separate environmental
sensor, not shown, embedded in the cassette 510 to track humidity or temperature
conditions in storage, transit, and in actual use which would determine if the
"warranty" is still valid for the printing toner/cassette. Another type of physical
identification device is a read-only type having a bar-code, dot-code, or a laser-
readable label.

Detailed Description Text (62):
The second system element required to facilitate pay-per-use transactions is an
RFID reader device 508, 522. A suitable RFID reader device 508, 522 reads the
electronic identification code(s) for the user, refurbisher, third-party service
provider, etc., along with the toner consumption, usage, pages printed or
reproduced, transmitted, refurbishing cycles, software or algorithm configuration,
billing rate, etc. type business transaction data. The foregoing information is
stored on the cassette RFID device 512 itself and/or a plug-in mass-memory card 516
in the peripheral 506. This RFID reader device 512 is preferably embedded in the
following equipment elements: (1) system peripherals such as printers, copiers,
facsimile machines, scanners, etc.; (2) printing cassette refurbishing/recycling
equipment 518; (3) portable, hand-held readers, notebook/sub-notebook computers,
terminals; (4) portable pagers; and (5) Portable Personal Digital Assistants (PDA)
or integrated computing/communicating.

Detailed Description Text (74):
In FIG. 6, this specific application is illustrated. In use, a sender is equipped
with an RFID badge 618. RFID badge 618 may be of the type discussed earlier in
Example 1 and in Example 2; therefore, RFID badge 618 may be independently powered
or may accumulate energy from interrogation transmissions from portable, equipment-
embedded RFID reader 602.

Detailed Description Text (76):
In use, a sending individual equipped with RFID badge 618 is passively identified
and activated (IDed) via Reader (RFID) in multi-media device 610. Upon activation,
RFID reader 602 performs a handshake sequence with RFID badge 618. This may be
accomplished by a plug-in card type RFID reader 606 embedded in the fixed base
unit/charger, wherein RFID reader 606 is similar to that described earlier in
example 2. Local host or server stored "digital voice signature" verification and

authorization can also be deployed to provide additional security over the
automatic RFID handshake sequence.

Detailed Description Text (77):
During the handshake sequence, plug-in card 606 may consult a local look-up table
contained therein; alternatively, plug-in card 606 may verify the authorization of
RFID badge 618 by communicating via antenna 604 of controller unit 603 to
transaction data base 620 maintained in LAN network equipment types via wired or
cellular communication. Transaction data base 620 is a generic term which
encompasses a network server/host or a central office switch of a local telephone
company, or a base/relay station within the local wired (PSTN) or cellular
telephone network or the like. Transaction data base 620 verifies the authorization
of RFID badge 618 and transmits same via cellular technology to controller unit 603
via controller unit antenna 604. Upon receipt of authorization, controller unit 603
allows multi-media device 610 to be activated.

Detailed Description Text (78):
The sender, now authorized, inputs the receiving individual's phone number or other
identification to initiate a communications link with a receiving individual
wearing RFID bade 622.

Detailed Description Text (79):
To establish the link, controller unit 603 passes the request to transaction data
base 620. Transaction data base 620 evaluates whether sender with RFID badge 618 is
authorized to communicate with recipient with RFID badge 622. Once authorized,
transaction data base 620 establishes a link with receiving multi-media devices
shown generally at 624.

Detailed Description Text (81):
When receiving multi-media device rings (or beeps, or a light blinks, etc.)
recipient having RFID badge 522 activates multi-media device 624. As soon as
recipient having RFID badge 622 activates multi-media device 624, a plug-in card or
RFID reader module 606 of receiving controller unit 603 interrogates RFID badge 622
to verify that the intended recipient is indeed receiving the communication.

Detailed Description Text (82):
Controller unit 603 may also be equipped with a GPS position card 608. It should
also be noted that an additional level of security may be afforded by use of GPS
position card 608 shown inserted into controller 603 although it may alternatively
be fixed to multi-media devices 610 and 624. Position card 608 may be interrogated
by or otherwise programmed to automatically broadcast or transmit location
information to) transaction data base 620 to verify whether either the sender or
recipient is in an authorized, predetermined, or dynamically programmed location.

Detailed Description Text (86):
As various modifications could be made in the constructions and methods herein
described and illustrated without departing from the scope of the invention, it is
intended that all matter contained in the foregoing description or shown in the
accompanying drawings shall be interpreted as illustrative rather than limiting.
For example, the concept presented in example 2 may be extended to track hazardous
waste (nuclear, chemical, medical) products by attaching a user RFID badge waste
handlers, equipments to each hazardous waste container to verify proper storage,
movement, handling, and disposal. Eliminating the "person-in-the-loop" is
advantageous because it reduces the potential for inadvertent exposure while
providing continuous surveillance over a large number of hazardous waste storage
containers. In another example of the scope of the present invention, it is
contemplated that an application-specific memory (ASM) device may also be
incorporated into the system to let the user, OEM, or service-provider collect data
in unique formats, frequency and storage patterns so as to minimize the data
"access time" and optimize output formats for statistical analysis purposes. In yet

another example, it is contemplated that the foregoing Example 4 may be extended to video-phone, video-conferencing, and voice-mail systems. It is further pointed out that the present invention could eliminate the need for an individual to remember passwords prior to logging on to a computer station by performing security functions transparent to the individual. In yet another example, FIG. 7 shows a computer managed system currently under development by the Microsoft Corporation. The present invention may be utilized in conjunction with the planned system disclosed in FIG. 7 to provide a comprehensive information management and security dimension consistent with the various embodiments of the present invention described above. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims appended hereto and their equivalents.

Other Reference Publication (9):
Standard Register, Advertisement--High Tech Document Security Video, Jul.-Aug. 1993.

CLAIMS:

1. An information management and security system comprising:

a transponder having an identification code, said transponder including a charge storage element for storing energy received from an interrogation signal, said transponder subsequently using the stored energy to power the transmission of said identification code;

an transceiver to send said interrogation signal to said transponder and to receive said identification code from said transponder;

a first terminal device connected to and activated by said transceiver;

a host network element in communication with said transceiver, said host network element having authorized identification codes stored in memory, whereby said host network element compares the identification of said transponder with the authorized identification codes stored in memory; and

a second terminal device connected to said host network element for communicating with said first terminal device after said host network element has verified the authorized identification of said transponder.

2. An information management and security system as set forth in claim 1, wherein prior to allowing communication between said first terminal device and said second terminal device said transceiver interrogates said transponder which causes said transponder to respond by broadcasting identification signals so that said transceiver receives the identification signals and communicates the identification signals to said host network element which authenticates the authorization of said transponder by comparing the identification signals with said authorized identification codes stored in said memory of said host network element.

3. An information management and security system as set forth in claim 1, wherein said transponder comprises a Personal Computer card having an transponder, mass memory, and input/output data means.

4. An information management and security system as set forth in claim 3, wherein said mass memory of said transponder is application specific memory.

5. Information management and security system as set forth in claim 1 wherein said transponder comprises an RF transponder.

6. An information management and security system as set forth in claim 3, wherein said transponder further comprises a battery power source.

7. An information management and security system as set forth in claim 1, wherein said transceiver writes a record of the transaction on said transponder.

8. An information management and security system as set forth in claim 3, wherein said transponder further comprises encryption means to encrypt signals emitted from said transponder.

9. An information management and security system as set forth in claim 8, wherein said encryption means comprises a random number seeding.

10. An information management and security system as set forth in claim 9, wherein said encryption means further comprises an encryption chip.

11. An information management and security system as set forth in claim 3, wherein said encryption means further comprises an integrated encryption and packetization chip.

12. An information management and security system as set forth in claim 1, wherein said transponder stores unique biographical information of a user of said transponder in Read Only Memory.

13. An information management and security system as set forth in claim 1, wherein said transceiver connected to said first terminal device writes the transaction on said singular transponder.

14. An information management and security system as set forth in claim 1, wherein said transceiver connected to said first terminal device stores a record of the transaction in memory.

15. An information management and security system as set forth in claim 1, wherein said transceiver connected to said first terminal device writes the transaction on said host network element.

16. An information management and security system as set forth in claim 1, wherein a request for a transfer of data between said first terminal and said second terminal is automatically stamped with the location, date and time of the request and stored in memory in said transceiver.

17. An information management and security system as set forth in claim 1, wherein said host network element records the identification communicated by said transponder.

18. An information management and security system as set forth in claim 1, wherein said transponder communicates with an environmental sensor.

19. An information management and security system as set forth in claim 18, wherein said environmental sensor detects an environmental condition selected from the group consisting of humidity, temperature, ozone, oxygen, and smoke particles.

20. An information management and security system as set forth in claim 1, wherein said first terminal device is selected from the group consisting of printers, copiers, pagers, personal digital assistants, personal computers, dumb terminals, workstations, facsimile machines, telephones, cellular phones, Video Cassette Recorders, radios, electronic door mechanisms, mass memory storage devices, data storage devices, automated teller machines, or modems.

21. An information management and security system as set forth in claim 1, wherein

said second terminal device is selected from the group consisting of printers, copiers, pagers, personal digital assistants, personal computers, dumb terminals, workstations, facsimile machines, telephones, cellular phones, Video Cassette Recorders, radios, electronic door mechanisms, mass memory storage devices, data storage devices, automated teller machines, or modems.

22. An information management and security system as set forth in claim 1, wherein said host network element is selected from the group consisting of network servers, network controllers, central office switches, or base relay stations.

23. An information management and security system as set forth in claim 20, wherein said second terminal device is selected from the group consisting of printers, copiers, pagers, personal digital assistants, personal computers, dumb terminals, workstations, facsimile machines, telephones, cellular phones, Video Cassette Recorders, radios, electronic door mechanisms, mass memory storage devices, data storage devices, automated teller machines, or modems.

24. Information management and security system as set forth in claim 1 wherein said transponder comprises an optical transponder.

25. Information management and security system as set forth in claim 1 wherein said transponder comprises an infrared transponder.

26. Information management and security system as set forth in claim 1 and further comprising a third terminal device connected to said host network element for communicating with said first terminal device after said host network element has verified the authorized identification of said RFID transponder.

27. An information management and security system comprising:

a first security badge including a transponder, a mass memory and an input/output circuit;

a first transceiver to wirelessly send and receive signals to and from said first transponder, said first transceiver to continuously transmit a broadcast signal until receiving a response from said first security badge and then, upon receipt of said response, said transceiver to receive a first authorization code from said first security badge and to store a record of the receipt of the authorization code;

a first terminal device connected to and activated by said first transceiver;

a second security badge including a transponder, a mass memory and an input/output device;

a second transceiver to send and receive signals to and from said second RFID transponder, said second transceiver to continuously transmit a broadcast signal until receiving a response from said second security badge and then, upon receipt of said response, said second transceiver to receive a second authorization code from said second security badge and to store a record of the receipt of the authorization code;

a second terminal device connected to and activated by said transceiver; and

a host network element in communication with said first transceiver and said second transceiver, said host network element to receive the first authorization code from the first transceiver and the second authorization code from the second transceiver and compare the first and second authorization codes with at least one host authorization code, said host network element to send a first verification code to the first transceiver upon verification of the first authorization code and to send

a second <u>verification</u> code to the second transceiver upon <u>verification</u> of the second authorization code.

28. A method of securing <u>access</u> to a terminal device, said method comprising the steps of:

providing an authorized user with a <u>security</u> badge which includes a personal computer card, a read/write transponder, a mass memory and a input/output data circuit, said transponder electronically storing an identification code; and

associating a transceiver with said terminal device, said transceiver being operable to communicate with said terminal device;

wherein said authorized user gains <u>access</u> to said terminal device by:

(a) bringing said <u>security</u> badge within a selected distance of said transceiver, said <u>security</u> badge located so that it is not physically visible so that said transponder is not within line-of-sight with said transceiver;

(b) transmitting an interrogation signal from said transceiver;

(c) receiving said interrogation signal at said <u>security</u> badge and storing said interrogation signal within a charge storage device within said <u>security</u> badge;

(d) transmitting said identification code from said <u>security</u> badge to said transceiver wherein the transmitting is powered by energy derived from said charge storage device;

(e) receiving said identification code at said transceiver; and

(f) <u>verifying</u> said <u>identification</u> code; wherein steps (b)-(f) are performed without said transponder being physically visible.

31. A method of securely communicating information between two locations comprising:

requesting an information transfer from a first location to a second location;

interrogating a radio frequency identification (<u>RFID</u>) transponder at said second location from a radio frequency (RF) transceiver at said second location;

transmitting an identification code from said <u>RFID</u> transponder at said second location to said RF transceiver at the said second location;

transmitting said identification code from said second location to a third location, said third location remote from said first and second locations;

comparing the authorization of said identification code with authorized identification codes stored in memory at said third location;

communicating an authorization signal from said third location; and

transmitting the requested information in packets to said second location after the authorization is <u>verified,</u> each of the packets of information including a header, the information to be transferred and a footer wherein the header includes an <u>identification</u> number for a user at the first location, an <u>identification</u> number for a receiver at the second location, a date/time stamp and a location stamp.

32. A method of securely communicating information between two locations comprising:

requesting an information transfer from a first location to a second location;

interrogating a radio frequency identification ("RFID") transponder at said first location from a radio frequency ("RF") transceiver at said first location;

transmitting an identification code from said RFID transponder at said first location to said RF transceiver at said first location;

transmitting said identification code from said first location to a third location, said third location remote from said first and second locations;

comparing the authorization of said identification code with authorized identification codes stored in a memory at said third location;

communicating an authorization signal from said third location; and

transmitting the requested information in packets to said second location after the authorization is verified, each of the packets of information including a header, the information to be transferred and a footer wherein the header includes an identification number for a user at the first location, an identification number for a receiver at the second location, a date/time stamp and a location stamp.

33. A method according to claim 32, wherein the step of transmitting the requested information to said second location after the authorization is verified, comprises the steps of:

storing the information requested for transfer in memory;

interrogating a radio frequency identification ("RFID") transponder at said second location from a radio frequency ("RF") transceiver at said second location;

transmitting an identification code from said RFID transponder at said second location to said RF transceiver at said second location;

comparing the authorization of said identification code with authorized identification codes stored in memory; and

transmitting the requested information to said second location after the authorization of the identification code of the RFID transponder at the second location is verified.

34. A method according to claim 33, wherein the step of transmitting the requested information to said second location after the authorization of the identification code of the RFID transponder at the second location is verified, comprises the step of:

transmitting the requested information to a terminal device at said second location, said terminal device being in communication with said RF transceiver at said second location.

38. A method according to claim 32, wherein the method further comprises the steps of:

encrypting the identification code transmitted from said RFID transponder; and

decrypting the identification code at said RF transceiver.

☐ [ Generate Collection. ]  [ Print ]

L55: Entry 14 of 14                    File: USPT        May 13, 1997

US-PAT-NO: 5629981
DOCUMENT-IDENTIFIER: US 5629981 A

TITLE: Information management and security system

DATE-ISSUED: May 13, 1997

INVENTOR-INFORMATION:

| NAME | CITY | STATE | ZIP CODE | COUNTRY |
|---|---|---|---|---|
| Nerlikar; Virupax M. | Plano | TX | | |

ASSIGNEE-INFORMATION:

| NAME | CITY | STATE | ZIP CODE | COUNTRY | TYPE CODE |
|---|---|---|---|---|---|
| Texas Instruments Incorporated | Dallas | TX | | | 02 |

APPL-NO: 08/ 283081    [PALM]
DATE FILED: July 29, 1994

INT-CL: [06] H04 L 9/00

US-CL-ISSUED: 380/25; 380/23, 340/825.34
US-CL-CURRENT: 713/168; 340/10.31, 340/10.32, 340/10.34, 340/10.41, 340/10.42, 340/10.51, 340/5.81, 380/243, 380/270, 705/75, 713/155

FIELD-OF-SEARCH: 380/23-25, 340/825.34

PRIOR-ART-DISCLOSED:

## U.S. PATENT DOCUMENTS

[ Search Selected ]  [ Search ALL ]  [ Clear ]

| | PAT-NO | ISSUE-DATE | PATENTEE-NAME | US-CL |
|---|---|---|---|---|
| ☐ | 4575621 | March 1986 | Dreifus | 380/23 |
| ☐ | 4691355 | September 1987 | Wirstrom et al. | 380/23 |
| ☐ | 4783798 | November 1988 | Leibholz et al. | 380/25 |
| ☐ | 4819267 | April 1989 | Cargile et al. | 380/23 |
| ☐ | 5053774 | October 1991 | Schuermann et al. | 342/44 |
| ☐ | 5153918 | October 1992 | Tuai | 380/25 |
| ☐ | 5310999 | May 1994 | Claus et al. | 380/23 |

☐  <u>5319711</u>      June 1994          Servi                    380/23

☐  <u>5339073</u>      August 1994        Dodd et al.              340/825.31

☐  <u>5508692</u>      April 1996         Wolfram                  380/23


## OTHER PUBLICATIONS

"Software Giant Aiming at the Office," New York Times, Jun. 8, 1993, p. C1.
Hardcopy Observer, Published by Lyra Research, "Microsoft at Work", vol. III, No.
7, Jul., 1993, pp. 31-39.
Hardcopy Observer, "Microsoft at Work to go Home?", vol. IV, No. 3, Mar., 1994, p.
9.
Hardcopy Observer, "Microsoft Gears Up to Supply at Work Print Software to OEM",
vol. IV, No. 2, pp. 30-32.
Fite, Jr., Franklin, "The PC Adopts an Embedded Position", Electronic Engineering
Times, Apr. 25, 1994, p. 46.
Wall Street Journal. William M. Bulkeley, "Get ready for the `smart cards` in
health care", May 1993, one page.
Wall Street Journal, John J. Keller, "Bells and whistles turn beepers into data
receivers", Sep. 1993 two pages.
Wall Street Journal, William M. Bulkeley, "Someday, Cards May Make Coins Obsolete
(smart cards may replace coin usage)", May 1993, one page.
Standard Register, Advertisement--High Tech Document <u>Security</u> Video, Jul.-Aug.
1993.


ART-UNIT: 422

PRIMARY-EXAMINER: Cangialosi; Salvatore

ATTY-AGENT-FIRM: Matsil; Ira S. Masterson; James C. Donaldson; Richard A.

ABSTRACT:

A closed loop, (networked) information management and <u>security</u> system which
provides a secure, end-to-end fully automated solution for controlling <u>access</u>
transmission, manipulation, and auditability of high value information comprising
an <u>RFID</u> transponder badge 302 and an RF reader transceiver 315 which is associated
with a host peripheral or a network. The RF reader transceiver 315 automatically
<u>identifies and verifies</u> authorization of the <u>RFID</u> transponder badge holder via a
"handshake" prior to allowing <u>access</u> to the host peripheral. The energy generated
by the transmission of the interrogation signal from the RF reader means 315
provides a power source which is accumulated and then used to activate a
transponder 304 response from the <u>RFID</u> transponder badge 302. The RF
reader/transceiver 315 writes the <u>access</u> transaction on either the <u>RFID</u> transponder
badge 302 and/or the host peripheral database or the network controller.
Alternatively, the RF reader means 315 may be associated via network server with a
LAN, WAN, or MAN. Optionally, an <u>RFID</u> badge 302a may be powered by an independent
power source such as a flatpak battery 314.

42 Claims, 10 Drawing figures

☐ [Generate Collection] [Print]

L55: Entry 14 of 14                    File: USPT            May 13, 1997

US-PAT-NO: 5629981
DOCUMENT-IDENTIFIER: US 5629981 A

TITLE: Information management and security system

DATE-ISSUED: May 13, 1997

INVENTOR-INFORMATION:

| NAME | CITY | STATE | ZIP CODE | COUNTRY |
|------|------|-------|----------|---------|
| Nerlikar; Virupax M. | Plano | TX | | |

ASSIGNEE-INFORMATION:

| NAME | CITY | STATE | ZIP CODE | COUNTRY | TYPE CODE |
|------|------|-------|----------|---------|-----------|
| Texas Instruments Incorporated | Dallas | TX | | | 02 |

APPL-NO: 08/ 283081    [PALM]
DATE FILED: July 29, 1994

INT-CL: [06] H04 L 9/00

US-CL-ISSUED: 380/25; 330/23, 340/825.34
US-CL-CURRENT: 713/158; 340/10.31, 340/10.32, 340/10.34, 340/10.41, 340/10.42, 340/10.51, 340/5.81, 380/243, 380/270, 705/75, 713/155

FIELD-OF-SEARCH: 380/23-25, 340/825.34

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

[Search Selected] [Search ALL] [Clear]

| | PAT-NO | ISSUE-DATE | PATENTEE-NAME | US-CL |
|---|--------|------------|---------------|-------|
| ☐ | 4575621 | March 1986 | Dreifus | 380/23 |
| ☐ | 4691355 | September 1987 | Wirstrom et al. | 380/23 |
| ☐ | 4783798 | November 1988 | Leibholz et al. | 380/25 |
| ☐ | 4819267 | April 1989 | Cargile et al. | 380/23 |
| ☐ | 5053774 | October 1991 | Schuermann et al. | 342/44 |
| ☐ | 5153918 | October 1992 | Tuai | 380/25 |
| ☐ | 5310999 | May 1994 | Claus et al. | 380/23 |

| | | | | |
|---|---|---|---|---|
| ☐ | 5319711 | June 1994 | Servi | 380/23 |
| ☐ | 5339073 | August 1994 | Dodd et al. | 340/825.31 |
| ☐ | 5508692 | April 1996 | Wolfram | 380/23 |

OTHER PUBLICATIONS

"Software Giant Aiming at the Office," New York Times, Jun. 8, 1993, p. C1.
Hardcopy Observer, Published by Lyra Research, 'Microsoft at Work', vol. III, No.
7, Jul., 1993, pp. 31-39.
Hardcopy Observer, "Microsoft at Work to go Home?", vol. IV, No. 3, Mar., 1994, p.
9.
Hardcopy Observer, "Microsoft Gears Up to Supply at Work Print Software to OEM",
vol. IV, No. 2, pp. 30-32.
Fite, Jr., Franklin, "The PC Adopts an Embedded Position", Electronic Engineering
Times, Apr. 25, 1994, p. 46.
Wall Street Journal. William M. Bulkeley, "Get ready for the 'smart cards' in
health care", May 1993, one page.
Wall Street Journal, John J. Keller, "Bells and whistles turn beepers into data
receivers", Sep. 1993 two pages.
Wall Street Journal, William M. Bulkeley, "Someday, Cards May Make Coins Obsolete
(smart cards may replace coin usage)", May 1993, one page.
Standard Register, Advertisement--High Tech Document Security Video, Jul.-Aug.
1993.

ART-UNIT: 222

PRIMARY-EXAMINER: Cangialosi; Salvatore

ATTY-AGENT-FIRM: Matsil; Ira S. Kesterson; James C. Donaldson; Richard L.

ABSTRACT:

A closed loop, (networked) information management and security system which
provides a secure, end-to-end fully automated solution for controlling access,
transmission, manipulation, and auditability of high value information comprising
an RFID transponder badge 302 and an RF reader transceiver 315 which is associated
with a host peripheral or a network. The RF reader transceiver 315 automatically
identifies and verifies authorization of the RFID transponder badge holder via a
"handshake" prior to allowing access to the host peripheral. The energy generated
by the transmission of the interrogation signal from the RF reader means 315
provides a power source which is accumulated and then used to activate a
transponder 304 response from the RFID transponder badge 302. The RF
reader/transceiver 315 writes the access transaction on either the RFID transponder
badge 302 and/or the host peripheral database or the network controller.
Alternatively, the RF reader means 315 may be associated via network server with a
LAN, WAN, or MAN. Optionally, an RFID badge 302a may be powered by an independent
power source such as a flatpak battery 314.

42 Claims, 10 Drawing figures